UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,185	07/24/2003	Mira Kristina LaCous	S30.12-0006	1550

27367 7590 06/23/2008
WESTMAN CHAMPLIN & KELLY, P.A.
SUITE 1400
900 SECOND AVENUE SOUTH
MINNEAPOLIS, MN 55402-3244

EXAMINER	
GERGISO, TECHANE	
ART UNIT	PAPER NUMBER
2137	
MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/626,185	LACOUS, MIRA KRISTINA	
	Examiner	Art Unit	
	TECHANE J. GERGISO	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12,14-22,35-39 and 41-51* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10, 12, 14-22, 35-39 and 41-51* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on March 04, 2008.

2. The applicant amended claims 1, 20, 22, 35, 49, added new claims 50, 5 and cancelled claims 17, 18, and 38.

3. Claims 1-10, 12, 14-22, 35-39 and 41-51 have been examined and are pending.

Specification

4. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 35-37, 39 and 41-48 recite "A **computer readable medium** having instructions stored thereon". The "**computer readable medium**" lacks proper antecedent basis in the specification.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 35-37, 39, 41-48 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 35 recites "A **computer readable medium** having instructions stored thereon…". However, the applicant has **not provided an explicit and deliberate** (i.e. limiting) definition for

"A computer readable medium" in the specification or limiting claim language. Claim 35 would be directed to an appropriate Manufacture within the meaning of 101 **if** the medium would only reasonably be interpreted by one of ordinary skill in the art as covering embodiments which are **articles produced from raw or prepared materials and which are structurally and functionally interconnect to the program in such a manner as to enable the program to act as a computer component and realize its functionally**. The "**computer-readable medium**" in claim 35 would suggest to one of ordinary skill signals or other forms of propagation and transmission media, typewritten or handwritten text on paper, or other items failing to be an appropriate manufacturer under 35 USC 101 in the **context of computer-related inventions**. Therefore, Claim 35 is rejected under 101 as failing to be limited to embodiments which fall within a statutory category. Claims 36-37, 39, 41-48 are also rejected under 101 as failing to be limited to embodiments which fall within a statutory category based on their dependency from claim 35.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites "*wherein making a determination comprises comparing a session number received with or as part of the biometric information packet to the record of the session number*." The "*record of the session number*" is **stored on the computing device and not on the biometric device**. It is not clear how the biometric device is comparing a session number received from the computing device and with "the record of session number" stored on the computing device or at least there might be an essential missing steps which is not claimed to enable the comparison. Therefore, the step of comparing "the session number" is not clear and renders the claim ambiguous to define its boundary and scope and rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Response to Arguments

9. Applicant's arguments filed March 04 have been fully considered but they are not persuasive.

The applicant argues that "the biometric device that collects a collection of biometric data has an encryption component as firmware that is related to the encryption component in the computing device that selectively utilizes the collection of biometric data. In both the Ting and Michener systems, biometric information is collected by a large number of client computers and is sent to a general use, large scale server. The large scale server in each system that uses the biometric information does not have encryption components that are related to each of the large number of clients that collect and send the biometric information." The examiner disagrees with

the applicant's argument and analysis for two reasons. First, Michener discloses a biometric device that collects a collection of biometric data has an encryption component as firmware that is related to the encryption component in the computing device. The teaching is disclosed in the trusted authorization device of figure 1, using trusted control processor, including a crypto chip (item 44) and firmware keys (item 26). Second, it is well known to one of ordinary skill in the art at the time of the invention to implement encryption modules using hardware, software or firmware or combination of them.

The examiner disagrees with the applicant argument that "In both the Ting and Michener systems, biometric information is collected by a large number of client computers and is sent to a general use, large scale server" because at least figure 1 of Michener has only one trusted authorization device including one trusted biometric input and relating to one of clients station 12 (each TAD service as a biometric device and each client service as computing device).

The examiner also disagrees with the applicant's argument that "the limitation that the steps of claim 1 be performed in the consecutive order of pre-establishing, generating, maintaining, encrypting, and receiving and applicant respectfully contends that Ting does not disclose the consecutive steps." During examination, the examiner considered sequence of order of the steps are inherent for example, encrypting packet is inherent to transmit the an encrypted packet, Transmitting the encrypted packet is inherent to receive the encrypted packet, receiving the encrypted packet is inherent to decrypt the encrypted and transmitted packet. Therefore, [pre-establishing, generating, mainlining , encrypting, transmitting , receiving and decrypting are

inherently sequentially ordered steps unless otherwise the applicant enables and establishes why and how the steps are not inherently sequenced order.

For the above reasons, the applicant's argument is not persuasive to overcome the prior arts in record and place independent claims 1, 35 and 49 in condition for allowance. Dependent claims 2-10, 12, 14-22, 36-39 and 41-48 and 50-51 depending directly or indirectly from their corresponding independent claims are also not placed in condition for allowance based on their dependency.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1-10, 12, 14-22, 35-39 and 41-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ting (US Pat. No. 2002/0174344) in view of Michener et al. (hereinafter referred to as Michener, US Pat. No. 7, 028, 191).

As per claim 1:

Ting discloses a computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

pre-establishing an encryption relationship between a computing device and the biometric device, wherein the computing device and biometric device include separate but related encryption components and decrypts information encrypted by the computing device encryption component (0013);

a session packet, and transmitting it to the biometric device wherein a session packet comprises generating a session number and storing it in the session packet (0025; 0029-31); and

receiving a biometric information packet from the biometric device, decrypting it, and making a determination, as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet, wherein making a determination comprises comparing a session number received with or a part of the biometric information packet to the record of the session number (0010; 0035; 0036).

Ting discloses does not explicitly teach encrypting the generated session packet utilizing the computing device encryption component and maintaining a record of the session number and the biometric device encryption component is implemented as firmware. Michener, in an analogous art, however teaches encrypting the generated session packet utilizing the computing device encryption component and maintaining a record of the session number and the biometric device encryption component is implemented as firmware (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60; figure 1: 44). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Ting to include encrypting the generated session packet utilizing the computing device encryption component and maintaining a record of the session

number and the biometric device encryption component is implemented as firmware. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 2:

Ting discloses a method, the consecutive order of pr-establishing, generating, maintaining, encrypting, and receiving (0030; 0036; 0039; ; order of the steps are inherent for example, encrypting packet and then transmitting the encrypted packet and then receiving the encrypted packet and then decrypting the encrypted and received packet is inherently orderly sequenced).

As per claim 3:

Michener discloses a method, further comprising storing the session number in a database associated with the computing device (Column 4: lines 52-65; Each TAD 10 is provided with a unique alphanumeric ID (TADID_A) and a unique and well-protected binary ID (TADID_B), each of which are stored in memory 26. Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 4:

Michener discloses a method, wherein generating a session packet comprises obtaining a session key and storing it in the session packet (column 7: lines 10-30; column 9: lines 1-30).

As per claim 5:

Michener discloses a method, further comprising storing the session key in a database associated with the computer (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 6:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption key that is complimentarily related to the session key (figure 10: 104, 1008, 1010; column 13: 54-65; column 15: lines 5-10, lines 16-23).

As per claim 7:

Michener discloses a method, wherein obtaining a session key comprises generating a public key portion of a PKI key pair (column 17: lines 5-11).

As per claim 8:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair (column 17: lines 5-11).

As per claim 9:

Michener discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with an encryption component that is independent of the pre-established encryption relationship (figure 17).

As per claim 10:

Michener discloses a method, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet (figure 13).

As pr claim 12:

Michener discloses a method, further comprising storing the session number, the session key and a session time stamp in a database associated with the computer (figure 17).

As per claim 14:

Michener discloses a method, wherein making a determination comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 55-60; figure 17).

As per claim 15:

Michener discloses a method, wherein making a determination comprises comparing a data representation of a user's biometric information to at least one data representation of biometric information stored in a database (column 5: lines 20-40).

As per claim 16:

Michener discloses a method, wherein making a determination comprises: comparing a session number to a list of valid values (column 9: lines 5-35); evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 55-60; figure 17); and comparing a database representation of a user's biometric information to at least one data representation of biometric information stored in a database (figure 17; column 9: lines 5-35; column 5: lines 20-40).

As per claim 19:

Michener discloses a method, wherein pre-establishing an encryption relationship comprises storing a first part of a PKI key pair with the computing device and a second part of the PKI key pair with the biometric device (figure 10: 1002-1022; abstract).

As per claim 20:

Michener discloses a method, wherein encrypting the session packet comprises encrypting the session packet utilizing the first parts of the PKI key pair (figure 10: 1002-1022; abstract).

As per claim 21:

Michener discloses a method, wherein pre-establishing an encryption relationship comprises storing a first part of a static encryption key pair with the computing and a second part of the static encryption key pair with the biometric device, one of the first and second parts being configured to decrypt information that has previously been encrypted utilizing the other part (figure 10: 1002-1022; abstract).

As per claim 22:

Michener discloses a method, wherein encrypting the session packet comprises encrypting the session packet utilizing the first part of the static encryption key pair (figure 10: 1002-1022; abstract).

As per claim 35:

Ting discloses a computer readable medium having instructions stored thereon which, when executed by a computing device, cause the computing device to perform a series of steps comprising:

first, receiving a session initiation command (0025; 0029-31);

fourth, transmitting the encrypted session packet to a biometric device; a session packet comprises obtaining a session key and storing it in the session packet (0025; 0029-31);

fifth, receiving a biometric information packet from the biometric device (0025);

six, decrypting the biometric information packet, wherein decrypting the biometric information packet comprises decrypting it with an encryption key that is complementary related to the session key (0010; 0035; 0036);

seventh, determining, based on a content of a collection of authentication information contained in the decrypted biometric information packet, whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet (0010; 0035; 0036); and

wherein first, second, third, fourth, fifth, six, and seventh respectively correspond to the consecutive order of the series of steps (0030; 0036; 0039; Figure 2: step 202-255; order of the steps are inherent for example, encrypting packet and then transmitting the encrypted packet and the receiving the encrypted packet and then decrypting the encrypted and received packet is inherently orderly sequenced).

Ting discloses does not explicitly teach encrypting the generated session packet and maintaining a record of the session number. Michener, in an analogous art, however teaches encrypting the generated session packet and maintaining a record of the session number (column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Ting to include encrypting the generated session packet and maintaining a record of the session number. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent

protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 36:

Michener discloses a computer readable medium, wherein generating a session packet comprises generating a session number and storing it in the session packet (column 9: lines 5-40; Session-Random Number).

As per claim 37:

Michener discloses a computer readable medium, further comprising the step of storing the session number in a database associated with the computing device (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 39:

Michener discloses a computer readable medium, further comprising the step of storing the session key in a database associated with the computer (Column 10: lines 1-25; figure 13: Table Lookup; data structure).

As per claim 41:

Michener discloses a computer readable medium, wherein obtaining a session key comprises generating a public key portion of a PKI key pair (column 17: lines 5-11).

As per claim 42:

Michener discloses a computer readable medium, wherein decrypting the biometric information packet with an encryption key that is complementary related to the session key comprises decrypting the biometric information packet with a private key portion of the PKI key pair (column 17: lines 5-11).

As per claim 43:

Michener discloses a computer readable medium, wherein generating a session packet comprises generating a session time stamp and storing it in the session packet (figure 13).

As per claim 44:

Michener discloses a computer readable medium, wherein determining comprises comparing a session number to a list of valid values (column 9: lines 5-35).

As per claim 45:

Michener discloses a computer readable medium, wherein determining comprises evaluating a session time stamp to determine whether the biometric information packet was received within a predetermined time period (column 2: lines 15-60; figure 17).

As per claim 46:

Michener discloses a computer readable medium, wherein encrypting the session packet comprises encryption the session packet with a first encryption component that is complimentarily related to a second encryption component maintained on the biometric device, one of the first and second encryption components being configured to decrypt information that has previously been encrypted utilizing the other of the first and second encryption components (figure 8: 802-808; figure 10: 1002-1012; abstract).

As per claim 47:

Michener discloses a computer readable medium, wherein the first and second encryption components are a PKI key pair (figure 10: 1002-1022; abstract).

As per claim 48:

Michener discloses a computer readable medium, wherein the first and second encryption components are a static encryption key pair (figure 10: 1002-1022; abstract).

As per claim 49:

Ting discloses a computer-implemented method for enhancing the security of informational interactions with a biometric device, comprising:

First, pre-establishing an encryption relationship between a computing device and the biometric, wherein pre-establishing an encryption relationship comprises storing a first encryption component with the computing device and a second encryption component with the biometric device, one of the first and second encryption components being configured to

decrypt information that has previously been encrypted utilizing the other of the first and second encryption components (0013);

Second, a session packet, and transmitting it to the biometric device wherein a session packet comprises generating a session number and storing it in the session packet (0025; 0029-0031);

Fourth, receiving from the biometric device a biometric information packet that is encrypted utilizing the session encrypted key, decrypting the biometric information packet with an encryption key that is complimentarily related to the session encryption key, and making a determination, as to whether or not to utilize a collection of biometric data contained in the decrypted biometric information packet based on a content of a collection of authentication information contained in the decrypted biometric information packet, wherein making a determination comprises comparing a session number received with or a part of the biometric information packet to the record of the session number (0010; 0035; 0036).

wherein first, second, and fourth respectively correspond to the consecutive order of the series of steps (0030; 0036; 0039; Figure 2: step 202-255; order of the steps are inherent for example, encrypting packet and then transmitting the encrypted packet and the receiving the encrypted packet and then decrypting the encrypted and received packet is inherently orderly sequenced).

Ting discloses does not explicitly teach encrypting the generated session packet. Michener, in an analogous art, however teaches encrypting the generated session packet

(column 4: lines 55-67; column 5: lines 40-67; figure 5a, 5b; column 7: lines 15-60). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Ting to include encrypting the generated session packet. This modification would have been obvious because a person having ordinary skill in the art would have been motivated by the desire a personal protection of electronic data that is small, easy to use, provides excellent protection to the PC/laptop use, that can operate in conjunction with corresponding devices at a central data gathering point to provide near real time validation of the information as suggested by Michener (in column 2: lines 55-62).

As per claim 50:

Ting discloses a method, wherein generating a session encryption key comprises generating a public key portion of a PKI key pair (0011; 0023).

As per claim 51:

Ting discloses a method, wherein receiving a biometric information packet and decrypting it comprises receiving a biometric information packet and decrypting it with a private key portion of the PKI key pair (0032-0034).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Contact Information

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Techane J. Gergiso whose telephone number is (571) 272-3784 and fax number is **(571) 273-3784**. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/T. J. G./

Examiner, Art Unit 2137

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2137